

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI**

**NICHOLAS SERVICES, LLC d/b/a
NICHOLAS AIR, AND NICHOLAS
JOHN CORRENTI,**

Plaintiffs,

v.

**CELLCO PARTNERSHIP,
d/b/a VERIZON WIRELESS**

Defendant.

CIVIL ACTION NO. 3:25-CV-117-DMB-JMV

COMPLAINT

Plaintiffs Nicholas Services, LLC, d/b/a Nicholas Air (or “Nicholas Air”) and Nicholas John Correnti (“Correnti”), by and through their undersigned counsel, allege as follows against Defendant Cellco Partnership, d/b/a Verizon Wireless (“Defendant” or “Verizon”).

I. INTRODUCTION

1. This lawsuit is a result of Verizon’s misfeasance, nonfeasance, and dereliction of its duties to protect Plaintiffs’ information security, privacy and identity, which resulted in the theft of \$500,000 (at the time of the theft) of cryptocurrency owned by Correnti (the “Crypto Theft”).

2. As set forth more fully herein, Verizon failed to protect Plaintiffs in accordance with its statutory and common law duties from being victimized by an unlawful SIM Swap caused by Verizon (the “SIM Swap”).

3. A “SIM Swap” enables an unauthorized third party to control a phone that appears to the wireless carrier network, and other servicers, to be that of the customer.

4. In a SIM Swap, the party in control of the phone has essentially “become” the person originally associated with that SIM card, cell phone, and cell phone account.

5. As a result of Verizon’s acts, omissions, and violations of its own stated policies and legal duties, Verizon allowed an unauthorized third party to steal approximately \$500,000 in various cryptocurrencies from Correnti, as an authorized user of the cell phone owned by Nicholas Air.

6. Plaintiffs bring this action to hold Verizon accountable for its wrongful conduct and other violations of federal and state law and to recover damages for breach of security and personal and financial harm suffered as a direct and proximate result of Verizon’s wrongful conduct, as well as failure to protect Plaintiffs’ information security, privacy and identity.

7. Plaintiffs seek compensatory damages, statutory damages, treble damages, restitution, disgorgement, punitive damages, attorneys’ fees, cost of suit, pre-judgment and post-judgment interest and such other and further relief as may be deemed proper.

II. THE PARTIES

8. Verizon is a telecommunications company incorporated in the state of Delaware.

9. Upon information and belief, Verizon’s headquarters are located at 1 Verizon Way, Basking Ridge, New Jersey 07920-1025.

10. Upon information and belief, Verizon is a wholly owned subsidiary of Verizon Communications, Inc.

11. Upon information and belief, Verizon is the business entity responsible for the provision of goods and services to the public, including Plaintiffs.

12. Accordingly, Verizon is the party with a relationship to Plaintiffs.

13. Verizon is a “common carrier,” as defined in the federal Telecommunications Act of 1996 (the “FCA”).

14. Verizon is subject to the FCA, the Federal Communication Commission (the “FCC”), and the regulations prescribed by the FCC.¹

15. Nicholas Air is a limited liability company organized under the laws of the State of Delaware, with its principal place of business in Oxford, Mississippi.

16. Correnti is, and at all relevant times was, a resident of Mississippi. Correnti currently resides in Oxford, Mississippi.

17. Plaintiffs established the Verizon account at issue on or about October 21, 2013.

III. JURISDICTION AND VENUE

18. Jurisdiction is proper in this Court pursuant to 28 U.S.C. § 1331 because this case concerns various federal questions under the FCA, the Stored Communications Act (the “SCA”), and the Computer Fraud and Abuse Act (the “CFAA”).

19. This Court has supplemental jurisdiction over Plaintiffs’ state law claims pursuant to 28 U.S.C. § 1367 because those claims share a common nucleus of operative facts with the federal claims.

20. This Court has personal jurisdiction over Verizon due to Verizon’s transaction of substantial business in Mississippi, purposeful direction of its conduct in Mississippi, maintenance of substantial aggregate contacts with Mississippi, and engagement in conduct that has a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons in Mississippi.

¹ See 47 C.F.R. § 64.2001 *et seq.*

21. Verizon has also purposefully availed, and continues to avail, itself of the laws of Mississippi by providing goods and services for sale to Mississippi citizens both online and through myriad physical stores operating within the state.

22. The cell phone and Verizon account at issue were purchased and established in Mississippi.

23. Plaintiffs were injured in Mississippi by the acts and omissions alleged herein.

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in the Northern District of Mississippi, and Verizon conducts business in this District. Plaintiffs were harmed in this District by Verizon's acts and omissions, as detailed further herein.

IV. STATEMENT OF CLAIMS

A. GENERAL BACKGROUND

25. Participation in modern society effectively requires the use of a smartphone to manage business, personal and financial affairs.

26. Activation and use of a smartphone, however, requires the engagement of a wireless carrier to provide service.

27. Verizon is one of the largest wireless carriers in the United States and the world.

28. In return, Verizon is compensated handsomely for its service, to the tune of \$76.7 billion of wireless service revenue in 2023 alone.²

29. As a wireless carrier, Verizon is the sentinel charged with safeguarding its customers' sensitive, personal, and confidential and proprietary information from unauthorized access.

² <https://www.verizon.com/about/sites/default/files/4Q23-Earnings-Release-Final.pdf?msockid=3b47564cabdb60bf18ee436eaacc615a>

30. One of the most insidious forms of unauthorized access occurs when an unauthorized party gains access to a customer's SIM card.

31. A Subscriber Identity Module (SIM) card holds the information identifying a specific customer to the wireless carrier, and vice versa.

32. The SIM card is the skeleton key that gives an intruder nearly unfettered access to a customer's electronically stored business, personal and financial life. Verizon has a duty to hold the proverbial line against unauthorized access to customers' SIM cards, and in particular here, to guard against unauthorized access to Plaintiffs' SIM card.

33. Once an unauthorized party takes over a SIM card and effectuates a SIM Swap, the intruder essentially "becomes" the original customer and the cell phone user.

34. All communication meant for the real customer is routed to the intruder by virtue of the SIM Swap.

35. As is common in today's world, many services rely on a customer's cell phone as an added layer of security against unauthorized access.

36. Multi-factor authentication ("MFA") is generally regarded as effective, but the concept presupposes that a wireless carrier is doing its job of protecting its customers' identities.

37. This is precisely what Verizon did not do in this case, when it aided, abetted, and affirmatively allowed and performed the SIM Swap.

38. Plaintiffs relied on Verizon's vast resources and numerous privacy guarantees to safeguard their sensitive, personal, and confidential and proprietary information.

39. Verizon failed to carry out its statutory and common law duties to Plaintiffs, resulting in the Crypto Theft.

B. SIM SWAP

40. On or about October 31, 2022, Plaintiff Nicholas Air purchased the iPhone at issue in this matter (the “iPhone”) and entered into a contract with Verizon for a business account (the “Verizon Account”).

41. Plaintiff Correnti is the owner of Nicholas Air and an authorized user of the iPhone and Verizon Account.

42. Plaintiff Correnti was authorized to use the iPhone and Verizon Account for both business and personal purposes.

43. On or about February 22, 2023, Correnti funded his Coinbase account with \$500,000 for the purpose of acquiring and trading various cryptocurrencies.

44. After funding of the account, various cryptocurrencies were held in the Coinbase account.

45. In or around September 2023, an unauthorized person communicated with Verizon, and Verizon wrongfully granted access to and control over Plaintiffs’ SIM card, iPhone and Verizon Account to the unauthorized person.

46. Critical to any SIM Swap is the affirmative reassignment of the SIM card by the wireless carrier, and it requires the knowing participation of the wireless carrier, here, Verizon.

47. Verizon and/or its employee(s) or agent(s) willfully, knowingly, and wantonly effectuated the SIM Swap of the iPhone and Verizon Account, without Plaintiffs’ authorization or consent.

48. Verizon and/or its employee(s) or agent(s) did not take the required steps to verify the identity of the impersonator.

49. Had Verizon taken appropriate verification steps, it would have been evident that Plaintiffs did not authorize the SIM Swap.

50. The SIM Swap transferred Plaintiffs' iPhone, SIM card, and Verizon Account to an unauthorized third party, giving the perpetrator complete access to all of Plaintiffs' incoming data, texts, and phone calls associated with the iPhone and Verizon Account.

51. The perpetrator could also intercept communications and impersonate Plaintiffs with its newfound ability to defeat MFA controls and other verification methods with respect to third party vendors, services, and providers, including Coinbase.

52. The SIM Swap could not have occurred without Verizon's involvement.

53. During the SIM Swap, Verizon accessed the Verizon Account and authorized changes to it without Plaintiffs' consent.

54. Verizon also actively issued the SIM card to a wireless cellular phone that was not associated with Plaintiffs' Verizon Account and was not owned by Plaintiffs.

55. Verizon issued a new SIM card on the iPhone and Verizon Account also despite (a) no Nicholas Air authorized person being physically present or otherwise duly authenticated to authorize the swap; and (b) the iPhone not being physically present or otherwise duly identified for the swap.

56. While the perpetrator had control over the iPhone and Verizon Account, he/she used that control to access and reset the passwords for Plaintiff Correnti's Coinbase account to effectuate the Crypto Theft.

C. AFTERMATH OF THE SIM SWAP

57. On or about October 27, 2023, Plaintiffs became aware of the Crypto Theft.

58. Plaintiff Correnti opened a dispute with Coinbase to investigate the Crypto Theft.

59. On or about December 21, 2023, Coinbase informed Plaintiff Correnti that on or about September 18 and 19, 2023, over the course of multiple transactions, the cryptocurrency assets had been transferred to external accounts outside his control.

60. Plaintiff Correnti reached out to Verizon to investigate the takeover of the iPhone and Verizon Account that facilitated the Crypto Theft.

61. Verizon represented to Plaintiffs via telephone that Plaintiffs were the victim of the SIM Swap.

62. Plaintiffs contacted the Federal Bureau of Investigation (FBI) to report the SIM Swap and Crypto Theft.

63. Plaintiffs suffered significant harm as a result of the SIM Swap, including unauthorized access to confidential and proprietary personal and company information and Plaintiff Correnti losing his entire Coinbase account balance.

64. Plaintiffs' highly sensitive and confidential business, personal and legal information was compromised as a result of the SIM Swap. Plaintiffs have been forced to spend a significant amount time and money to attempt to recover from the SIM Swap of the iPhone and Verizon Account, including recovery from identity theft.

V. CAUSES OF ACTION

**COUNT I
Violation of Telecommunications Act,
47 U.S.C. § 201 *et seq.***

65. Plaintiffs reallege and incorporate all of the preceding paragraphs as though fully set forth herein.

66. Verizon is a telecommunications carrier, or common carrier, engaged in interstate communication that furnishes communication services to the public.³

67. Verizon is subject to the FCA and has a duty to protect the confidentiality of the proprietary information of its customers, including Plaintiffs.⁴

68. The FCA also requires Verizon's practices related to the collection of information from its customers to be "just and reasonable" and declares unlawful any practice that is unjust or unreasonable.⁵

69. Under the FCA, Verizon must maintain the confidentiality of its customers' "Customer Proprietary Network Information" ("CPNI"), including Plaintiffs' CPNI.⁶

70. The FCC has promulgated rules to implement Section 222 of the FCA "to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI."⁷

71. In addition, the FCA "requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure."⁸

72. Carriers such as Verizon are liable under the FCA for failing to protect their customers' information from unauthorized use or disclosure.⁹

³ See 47 U.S.C. § 201(a).

⁴ 47 U.S.C. § 222(a).

⁵ 47 U.S.C. § 201(b).

⁶ 47 U.S.C. § 222(c); 47 U.S.C. § 222(h)(1) (defining CPNI as "(A) information that relates to the *quantity, technical configuration, type, destination, location, and amount of use* of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.").

⁷ 13 FCC Rcd. at 8195 ¶ 193; *see also* 47 C.F.R. § 64.2001 *et seq.*

⁸ Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 F.C.C. Rcd. 6927 ¶ 1 (April 2, 2007) (the "2007 CPNI Order").

⁹ 47 U.S.C. §§ 206, 207.

73. The FCC confirmed carriers' liability for such failures: "[t]o the extent that a carrier's failure to take reasonable precautions renders private customer information unprotected or results in disclosure of individually identifiable CPNI, . . . a violation of Section 222 may have occurred."¹⁰

74. The FCA also expressly authorizes private actions against common carriers that either (a) " . . . do, or cause or permit to be done" anything prohibited by the FCA, or (b) "omit to do" anything required by the FCA.¹¹

75. Verizon was required by the FCA to protect Plaintiffs' CPNI from unauthorized disclosure or use.

76. Verizon failed to do so when it effectuated the SIM Swap and failed to protect Plaintiffs' CPNI from unauthorized use or disclosure.

77. Verizon violated duties enumerated in 47 C.F.R. Subpart U by failing to establish and implement safeguards to prevent unauthorized use or disclosure of CPNI, maintain records with appropriate CPNI controls, and take other reasonable steps to guard against the kind of harm it facilitated by authorizing the SIM Swap.

78. The existence of a SIM swap security vulnerability has been widely known for years by mobile phone carriers such as Verizon. In June 2016, for example, the FTC's then Chief Technologist advised that "mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking . . . mobile carriers and third-party retailers need

¹⁰ Declaratory Ruling, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information & Other Customer Information*, 28 F.C.C. Rcd. 9609 ¶ 30 (2013) ("2013 CPNI Order").

¹¹ 47 U.S.C. §§ 206, 207.

to be vigilant in their authentication practices to avoid putting their customers at risk of major financial loss[.]”¹²

79. Further, researchers at Princeton University conducted an empirical study of wireless carriers’ SIM swap authentication procedures in 2020 (the results of which Verizon was aware of prior to publication) that found “five carriers in the United States continue to use authentication methods that are now known to be insecure, enabling straightforward SIM swap attacks” including Verizon.¹³

80. As a direct and proximate result of Verizon’s actions and failures to act, Plaintiffs suffered direct monetary damages in an amount of at least \$500,000.

WHEREFORE, Plaintiffs request that this Court enter judgment in their favor and against Verizon for (A) compensatory damages in the amount of at least \$500,000, or in such other amount as may be proven at trial; plus (B) pre-judgment interest; (C) post-judgment interest at the statutory rate; (D) costs and fees (including attorneys’ fees) incurred by Plaintiffs in this action; and (E) such other and further relief appropriate to the nature of Plaintiffs’ claims.

COUNT II
Violation of Stored Communications Act,
18 U.S.C. §2701 et seq.

81. Plaintiffs reallege and incorporate all of the preceding paragraphs as if fully set forth herein.

¹² Lorrie Cranor, *Your mobile phone account could be hijacked by an identity thief*, Tech@FTC (June 7, 2016), available at <https://www.ftc.gov/>, Mrs. Cranor also discussed her concerns about SIM swaps in her reply comments before the FCC in July 2016. *See In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunication Services*, WC Docket No. 16-106 (July 6, 2016).

¹³ Kevin Lee, et al., *An Empirical Study of Wireless Carrier Authentication for SIM Swaps*, IEEE TC on Security & Privacy (Nov. 18, 2024), <https://www.ieee-security.org/TC/SPW2020/ConPro/papers/lee-conpro20.pdf>.

82. Under the Stored Communications Act (“SCA”), “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.”¹⁴

83. None of the exceptions to the prohibitions set forth in Sections 2702(a)(1) and (2) are applicable to this case.

84. The SCA creates a private right of action for those “aggrieved by any violation” of its provisions.¹⁵

85. The conduct of Verizon, as alleged herein, constitutes a knowing and/or intentional violation of the SCA’s Section 2702(a).

86. The SIM Swap, at its core, necessitates the use of the SIM as “electronic storage” because its function as an identity authenticator is “temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission.”¹⁶

87. Verizon is a provider of remote computing services in connection with and in furtherance of the normal course of its wireless text and data service plans.

88. Plaintiffs have been “aggrieved” by the conduct of Verizon as alleged herein.

89. Pursuant to the applicable provisions of the SCA, Plaintiffs are entitled to actual and statutory damages, as well as reasonable attorneys’ fees and costs.¹⁷

WHEREFORE, Plaintiffs request that this Court enter judgment in their favor and against Verizon for (A) actual and statutory damages in the amount of at least \$500,000, or in such other amount as may be proven at trial; (B) pre-judgment interest; (C) post-judgment interest at the

¹⁴ 18 U.S.C. § 2702(a)(1).

¹⁵ 18 U.S.C. § 2707(a).

¹⁶ 18 U.S.C. § 2510(17).

¹⁷ 18 U.S.C. § 2707(c).

statutory rate; (D) costs and fees (including attorneys' fees) incurred by Plaintiffs in this action; and (E) such other and further relief appropriate to the nature of Plaintiffs' claims.

COUNT III
Violation of Computer Fraud and Abuse Act,
18 U.S.C. § 1030

90. Plaintiffs reallege and incorporate all of the preceding paragraphs as if fully set forth herein.

91. The CFAA governs those who intentionally access computers without authorization or who intentionally exceed authorized access and, as a result of such conduct, cause damage and loss.

92. A cell phone is a "computer" within the meaning of the CFAA.¹⁸

93. As set forth in the CFAA, the term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser [sic] is not entitled so to obtain or alter."¹⁹

94. As alleged herein, a SIM swap scam requires intentional access to customer computer data by Verizon that exceeds its authority and has caused damage and loss.

95. Verizon is subject to the provisions of the CFAA.

96. Verizon's conduct, as alleged herein, constitutes an intentional violation of Section (a)(5)(A) and Section (a)(5)(C) of the CFAA.

97. Verizon intended to engage in the SIM card reassignment associated with Plaintiffs' iPhone and Verizon Account.

98. Verizon is also liable for the acts, omissions, and/or failures, as alleged herein, of any of its officers, employees, agents, or any other person acting for or on behalf of Verizon.

¹⁸ See 18 U.S.C. § 1030(e)(1).

¹⁹ See 18 U.S.C. § 1030(e)(6).

99. Verizon violated the CFAA by exceeding its authority to access the computer data and breaching the confidentiality of the personal and proprietary information of Plaintiffs by using, disclosing, or permitting access to Plaintiffs' CPNI without the consent, notice, and/or legal authorization as required by the CFAA.

100. Section 1030(g) of the CFAA authorizes a private right of action for anyone that "suffers damage or loss by reason of a violation of this section . . . to obtain compensatory damages and injunctive relief or other equitable relief."

101. Plaintiffs suffered aggregate consequential damages which exceed the threshold of \$5,000 as required by Section 1030(c)(4)(A)(i)(I) of the CFAA.

102. Plaintiffs suffered a cognizable loss under the CFAA due to the expenses incurred in restoring lost SIM card access, loss of at least \$500,000 in Plaintiff Correnti's Coinbase account, tracing and attempting to regain possession of the assets lost in the Crypto Theft, and taking such other and further measures necessary to restore the iPhone, Verizon Account, Coinbase account, and Plaintiffs' identity.

WHEREFORE, Plaintiffs request that this Court enter judgment in their favor and against Verizon for (A) consequential damages in such amount as may be proven at trial; (B) pre-judgment interest; (C) post-judgment interest at the statutory rate; and (D) such other and further relief appropriate to the nature of Plaintiffs' claims.

COUNT IV
Violation of the Mississippi Constitutional Right to Privacy

103. Plaintiffs reallege and incorporate all of the preceding paragraphs as if fully set forth herein.

104. Article 3, Section 32 of the Mississippi Constitution of 1890, mirroring the Ninth Amendment to the United States Constitution, declares: "The enumeration of rights in this

constitution shall not be construed to deny and impair others retained by, and inherent in, the people.”

105. The right to privacy is retained by, and inherent in, the people.

106. “[P]rivacy is the ‘most comprehensive and guarded right emanating from the Mississippi Constitution,’ . . . and ‘the right most valued by civilized man.’”²⁰

107. Plaintiffs had, and continue to have, a reasonable expectation of privacy in their mobile device, confidential, personal and proprietary information, and Verizon Account information.

108. Verizon intentionally intruded on and into Plaintiffs’ solitude, seclusion, or private affairs by allowing its employees and unauthorized third parties to improperly access Plaintiffs’ confidential, personal and proprietary iPhone and Verizon Account information without proper consent or authority.

109. The reasonableness of Plaintiffs’ expectation of privacy is supported by Verizon and its agents’ unique position to safeguard Plaintiffs’ iPhone, SIM card, and Verizon Account information, including the sensitive, personal, confidential and proprietary information, and CPNI contained therein, and protect them from SIM Swap attacks.

110. Verizon and its agents’ intrusions into Plaintiffs’ privacy and failure to protect their identities are highly offensive to a reasonable person. Federal legislation enacted by Congress and rules promulgated and enforcement actions undertaken by the FCC aimed at protecting Verizon customers’ sensitive account data from unauthorized use or access underscore both the pervasiveness and awareness of the problem, as well as the magnitude of its offensiveness.

²⁰ *PHE, Inc. v. State of Mississippi*, 877 So. 2d 1244, 1248 (Miss. 2004) (internal citations omitted).

111. The offensiveness of Verizon's conduct is heightened by its material misrepresentations to Plaintiffs concerning the safety and security of the Verizon Account and the privacy and confidentiality of their associated information.

112. Plaintiffs suffered personal and financial harm by the intrusion into their private affairs, as detailed herein.

113. Verizon's actions and conduct were a substantial factor in causing the harm Plaintiffs suffered. But for Verizon employees' involvement in the SIM Swap, along with Verizon's failure to protect Plaintiffs from such harm through adequate security and oversight systems and procedures, Plaintiffs would not have had their privacy and security repeatedly violated, and Plaintiff Correnti would not have been a victim of the Crypto Theft.

114. Verizon's actions were malicious, oppressive, and willful. Verizon knew or should have known about the risks faced by Plaintiffs and the grave consequences of such risks. Nonetheless, Verizon failed in its duty to protect Plaintiffs. Punitive damages are warranted to deter Verizon from engaging in future misconduct.

WHEREFORE, Plaintiffs request that this Court enter judgment in their favor and against Verizon for (A) compensatory damages in the amount of at least \$500,000, or in such other amount as may be proven at trial; (B) punitive damages in amount to be determined at trial; (C) pre-judgment interest; (D) post-judgment interest at the statutory rate; and (E) such other and further relief appropriate to the nature of Plaintiffs' claims.

COUNT V (on behalf of Correnti)
Violation of the Mississippi Consumer Protection Act
Miss. Code § 75-24-1 *et seq.*

115. Plaintiff Correnti realleges and incorporates all of the preceding paragraphs as if fully set forth herein.

116. As Verizon customers, Plaintiffs engaged in transactions with Verizon concerning their wireless service. Plaintiffs sought and acquired services from Verizon for personal, family, business, and household purposes.

117. Verizon engaged in unfair methods of competition and unfair or deceptive acts or practices intended to result and which did result in the sale of wireless services to Plaintiffs, as detailed herein.

118. Verizon's acts and representations concerning the safeguards it employs to protect consumer account data, including Correnti's iPhone, SIM card, and Verizon Account information, are likely to mislead reasonable consumers, including Correnti.

119. Verizon represented that its goods or services are of a particular standard that, in actuality, they do not meet. Specifically, Verizon represented that, in purchasing Verizon wireless cell service and using Verizon-compatible phones, Correnti's personal and confidential data would be safeguarded and protected.

120. Verizon's wireless service did not protect and/or safeguard Correnti's personal, business, confidential and proprietary data from unauthorized access, and Verizon's employees allowed unauthorized access to Correnti's personal information.

121. Verizon's misrepresentations and omissions concerning its safeguarding of customer data were materially misleading, including to Correnti. As alleged above, a reasonable person would attach importance to Verizon safeguarding the privacy of his/her sensitive account data in determining whether to contract with a wireless cell phone provider, and Correnti did so in contracting with Verizon for the iPhone and Verizon Account.

122. Verizon was obligated to disclose the shortcomings of its data protection practices, as Verizon had exclusive knowledge of material facts not known or knowable to its customers.

Verizon actively concealed these material facts from its customers, including Correnti. Such disclosures were necessary to materially qualify its representations that it took measures to protect consumer data and its partial disclosures concerning its use of customers' CPNI. Further representations were necessary to prevent Verizon's statements from misleading the public and Correnti in light of the undisclosed facts concerning its security procedures.

123. Verizon's misrepresentations and failures to disclose information to Correnti constitute unfair and/or deceptive trade practices as defined in the Mississippi Consumer Protection Act.

124. Correnti was deceived by Verizon's unfair and deceptive trade practices.

125. Prior to filing this lawsuit, and in compliance with Miss. Code § 75-24-15, a complaint was filed on March 13, 2025 with the Mississippi Attorney General's Office (Reference Number 25-3530) constituting "a reasonable attempt to resolve [Correnti's] claim through an informal dispute settlement program approved by the Attorney General."

126. Despite his efforts to use the informal dispute settlement program, the Mississippi Attorney General's Office responded that "[Correnti] can continue working with the FBI, thanks."

127. Accordingly, Correnti brings this claim as part of the present lawsuit.

128. As a direct and proximate result of Verizon's unfair and deceptive trade practices, Correnti suffered harm.

WHEREFORE, Plaintiff Correnti requests that this Court enter judgment in his favor and against Verizon for (A) compensatory damages in the amount of at least \$500,000, or in such other amount as may be proven at trial; (B) pre-judgment interest; (C) post-judgment interest at the statutory rate; (D) reimbursement of its reasonable fees and costs (including attorneys' fees)

incurred in this action; (E) an Order enjoining Verizon from further violations of Mississippi and federal law; and (F) such other and further relief appropriate to the nature of Correnti's claims.

COUNT VI
Breach of Contract

129. Plaintiffs reallege and incorporate all of the preceding paragraphs as if fully set forth herein.

130. Plaintiffs and Verizon were parties to a valid, legally binding, and enforceable contract. A copy of the Verizon Customer Agreement is attached hereto as Exhibit 1 and incorporated by reference herein.

131. Verizon materially breached the Verizon Customer Agreement by failing to protect Plaintiffs' iPhone, SIM card, and Verizon Account information and CPNI, and permitting the SIM Swap and the resulting Crypto Theft of Plaintiff Correnti's Coinbase assets.

132. Plaintiffs performed all of their obligations under the Verizon Customer Agreement at the time of Verizon's material breach.

133. As a direct and proximate result of Verizon's various material breaches of the Verizon Customer Agreement, Plaintiffs suffered damages.

WHEREFORE, Plaintiffs request that this Court enter judgment in their favor and against Verizon for (A) compensatory damages in the amount of at least \$500,000, or in such other amount as may be proven at trial; (B) pre-judgment interest; (C) post-judgment interest at the statutory rate; and (D) such other and further relief appropriate to the nature of Plaintiffs' claims.

COUNT VII
Negligence

134. Plaintiffs reallege and incorporate all of the preceding paragraphs as if fully set forth herein.

135. Verizon owed Plaintiffs statutory and common law duties to secure the iPhone, SIM card and Verizon Account and to safeguard the confidential, personal and proprietary information therein.

136. This duty included, among other things, the duty to design, maintain, monitor, and test its own systems, protocols, and practices, and to monitor and test the systems, protocols, and practices of its agents, partners, and independent contractors, to ensure that Plaintiffs' information was adequately secured from unauthorized access.

137. Verizon owed a duty to Plaintiffs to disclose to them that its data security practices were inadequate to safeguard Plaintiffs' Verizon Account data from unauthorized access by its own employees and others.

138. Verizon also owed Plaintiffs a duty to properly hire, train, and supervise its employees.

139. Verizon had the unique ability to protect its systems and the data Verizon stored thereon from unauthorized access.

140. Plaintiffs' willingness to contract with Verizon, and thereby entrust Verizon with confidential, personal and other sensitive data, was predicated on Verizon undertaking adequate security and consent precautions and controls.

141. Verizon breached its duties to Plaintiffs by (a) failing to implement and maintain adequate security practices to safeguard the iPhone, SIM card, Verizon Account and data, including Plaintiffs' CPNI, from unauthorized access; (b) failing to detect unauthorized access in a timely manner; (c) failing to disclose that Verizon's data security practices were inadequate to safeguard Plaintiffs' data; (d) failing to supervise its employees and prevent employees from

improperly accessing and using Plaintiffs' iPhone, SIM card, Verizon Account and data without authorization; and (e) failing to provide adequate and timely notice of unauthorized access.

142. Verizon also breached its duty by failing to properly authorize a legitimate SIM swap, failing to properly verify the perpetrator's identity before facilitating the wrongful SIM Swap, and/or failing to prevent damages to Plaintiffs.

143. Neither Plaintiffs nor anyone else could facilitate the SIM Swap without Verizon's involvement.

144. Verizon knew or should have known that the unauthorized individual seeking to effectuate the SIM Swap was not Plaintiffs.

145. Verizon knew that Plaintiffs were Mississippi residents due to the address on the Verizon Customer Agreement and the usage data associated with the Verizon Account.

146. Nonetheless, Verizon effectuated the transfer of Plaintiffs' Verizon Account to a different cell phone and unauthorized third party.

147. Verizon should have insisted on stricter identity verification methods for a customer seeking to swap SIM cards – such as requiring the individual to provide photo identification – to insure that the swap was in fact authorized by the customer.

148. Additionally, the SIM Swap was foreseeable. Verizon knew or should have known that Plaintiffs' iPhone, SIM card, and Verizon Account were at risk due to the prevalence of SIM Swaps, yet it nonetheless failed to secure Plaintiffs' iPhone, SIM card, and Verizon Account and failed to properly supervise and train its employees.

149. Verizon has known for more than a decade that third parties frequently attempt to access wireless customers' accounts for fraudulent purposes. Indeed, Verizon has been sued in federal courts previously for similar unauthorized SIM card swaps.

150. In 2007, the FCC issued an order strengthening its CPNI rules in response to the growing practice of “pretexting.”²¹ Pretexting is “the practice of pretending to be a particular customer or authorized person to obtain access to that customer’s call detail or other private communication records.”²²

151. This 2007 Order was one of the methods by which Verizon was put on notice that its customers’ accounts were vulnerable targets of the third parties seeking unauthorized access.

152. Verizon also knew, or should have known, about the risk that SIM Swap crimes present to its customers. SIM swap crimes have been a widespread and growing problem for years.

153. Verizon knew or should have known that it needed to take steps to protect its customers from SIM Swaps and other account hijacks.

154. The FTC has confirmed that “mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking”²³ and urged carriers such as Verizon to “adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions.”²⁴

155. Verizon was, therefore, well aware of the significant risk that Verizon employees and SIM swapping presented to its customers, as well as the need to mitigate such risks, but it nonetheless failed to take adequate steps to protect Plaintiffs.

156. Plaintiffs, meanwhile, acted reasonably and with due care by taking the steps that Verizon authorized them to take in order to protect the iPhone and Verizon Account.

157. Verizon assured Plaintiffs that taking these steps would protect the iPhone and Verizon Account from breaches, such as SIM Swaps.

²¹ 2007 CPNI Order.

²² *Id.* at ¶ 1.

²³ *Id.* (emphasis added).

²⁴ *Id.*

158. At all relevant times, Verizon employees were acting within the scope of their employment.

159. Accordingly, Verizon is liable to Plaintiffs for the acts and omissions of those employees described herein.

160. As a direct and proximate result of Verizon's repeated breaches of its various duties to Plaintiffs, they suffered damages, including (without limitation) substantial monetary loss.

WHEREFORE, Plaintiffs request that this Court enter judgment in their favor and against Verizon for (A) compensatory damages in the amount of at least \$500,000, or in such other amount as may be proven at trial; (B) pre-judgment interest; (C) post-judgment interest at the statutory rate; and (D) such other and further relief appropriate to the nature of Plaintiffs' claims.

COUNT VIII Gross Negligence

161. Plaintiffs reallege and incorporate all of the preceding paragraphs as if fully set forth herein.

162. Verizon owed Plaintiffs a duty to properly handle and safeguard Plaintiffs' CPNI and access to the iPhone, SIM card, and Verizon Account.

163. Verizon was required to ensure its compliance with federal law and to protect the confidentiality of its customers' account data, including that of Plaintiffs.

164. Upon information and belief, Verizon willfully disregarded and/or showed reckless indifference to its duties under the common law and federal and state law to Verizon customers and to foreseeable victims of Verizon's wrongful acts, including Plaintiffs.

165. Having privileged and superior knowledge of prior account takeover attacks on Verizon customers' data and having the ability to leverage internal systems, procedures, and safeguard to prevent such attacks, Verizon nevertheless failed:

- a. to institute appropriate controls to prevent unauthorized access to customers' accounts, including Plaintiffs'; and
- b. to use authentication systems it knew or should have known were vulnerable to account takeover attacks; and
- c. by willfully disregarding the best practices of the industry in failing to implement systems to thwart such attacks; and
- d. to appropriately hire, retain, supervise, train, and control those officers, agents, and employees who could grant unauthorized access to customer account data.

166. Verizon's policies, procedures, and safeguard were ineffective and inadequate to prevent the unauthorized access to its customers' data, including Plaintiffs' data.

167. Verizon's actions, as alleged herein, evidence a carelessness that can only be characterized as a complete disregard for Plaintiffs' rights and the rights of Verizon's customers.

WHEREFORE, Plaintiffs request that this Court enter judgment in their favor and against Verizon for (A) compensatory damages in the amount of at least \$500,000, or in such other amount as may be proven at trial; (B) punitive damages in amount to be determined at trial; (C) pre-judgment interest; (D) post-judgment interest at the statutory rate; and (E) such other and further relief appropriate to the nature of Plaintiffs' claims.

COUNT IX

Negligent Hiring, Training, and/or Supervision

168. Plaintiffs reallege and incorporate all of the preceding paragraphs as though fully set forth herein.

169. Verizon conducts its business activities through employees or other agents.

170. The actions and omissions of Verizon employees, acting within the scope of their employment, proximately caused harm to Plaintiffs, as more fully described herein.

171. Verizon knew, or in the exercise of reasonable care and diligence should have known, that its employees could cause harm to Verizon's customers, including Plaintiffs.

172. Verizon breached its duty to Plaintiffs when it failed to exercise reasonable care in selecting, hiring, supervising, training, and retaining the employees and/or agents described in this Complaint.

173. Verizon breached its duties to Plaintiffs by hiring and retaining the employees and/or agents who participated in the SIM Swap that resulted in the Crypto Theft, breach of Plaintiffs' confidential, personal, business and proprietary data, and other damages to Plaintiffs.

WHEREFORE, Plaintiffs request that this Court enter judgment in their favor and against Verizon for (A) compensatory damages in the amount of at least \$500,000, or in such other amount as may be proven at trial; (B) pre-judgment interest; (C) post-judgment interest at the statutory rate; (D) such other and further relief appropriate to the nature of Plaintiffs' claims.

COUNT X
Negligent Misrepresentation

174. Plaintiffs reallege and incorporate all of the preceding paragraphs as if fully set forth herein.

175. As set forth above, Verizon owed Plaintiffs a duty to speak truthfully regarding (a) its ability and capacity to protect Plaintiffs' iPhone, SIM card, the Verizon Account, and CPNI, (b) the actions it took to protect Plaintiffs' iPhone, SIM card, the Verizon Account, and CPNI, and (c) breaches of Plaintiffs' iPhone, SIM card, the Verizon Account, and CPNI.

176. Verizon repeatedly represented to Plaintiffs, publicly and otherwise, that it could and would protect their personal and business information and account.

177. Verizon also represented to Plaintiffs that, if they took the steps that Verizon advised to protect the Verizon Account and information, they would be safe from incursion by unauthorized third parties.

178. These representations by Verizon regarding the security of Plaintiffs' iPhone, SIM card, the Verizon Account, and CPNI were material to their decision to establish and maintain service with Verizon.

179. Verizon's representations were materially false.

180. Verizon intended and knew that Plaintiffs would act or rely upon its misrepresentations.

181. Verizon knew that Plaintiffs would likely suffer harm by relying on its misrepresentations.

182. Plaintiffs reasonably relied to their detriment on Verizon's misrepresentations.

183. As a direct and proximate result of their reasonable reliance to their detriment on Verizon's misrepresentations, Plaintiffs suffered damages.

WHEREFORE, Plaintiffs request that this Court enter judgment in their favor and against Verizon for (A) compensatory damages in the amount of at least \$500,000, or in such other amount as may be proven at trial; (B) pre-judgment interest; plus (C) post-judgment interest at the statutory rate; plus (D) such other and further relief appropriate to the nature of Plaintiffs' claims.

VI. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury as to all issues so triable.

Respectfully submitted this 10th day of April, 2025.

/s/ Elizabeth B. Shirley

Elizabeth B. Shirley
(Fed. Bar No. BOSQE5958)
(MS Bar #100382)

Burr & Forman LLP
420 20th St. N
Suite 3400
Birmingham, AL 35203
Phone: (205) 251-3000
Fax: (205) 458-5100
E-mail: bshirley@burr.com

Attorney for Plaintiffs
Nicholas John Correnti and Nicholas Services, LLC
dba Nicholas Air